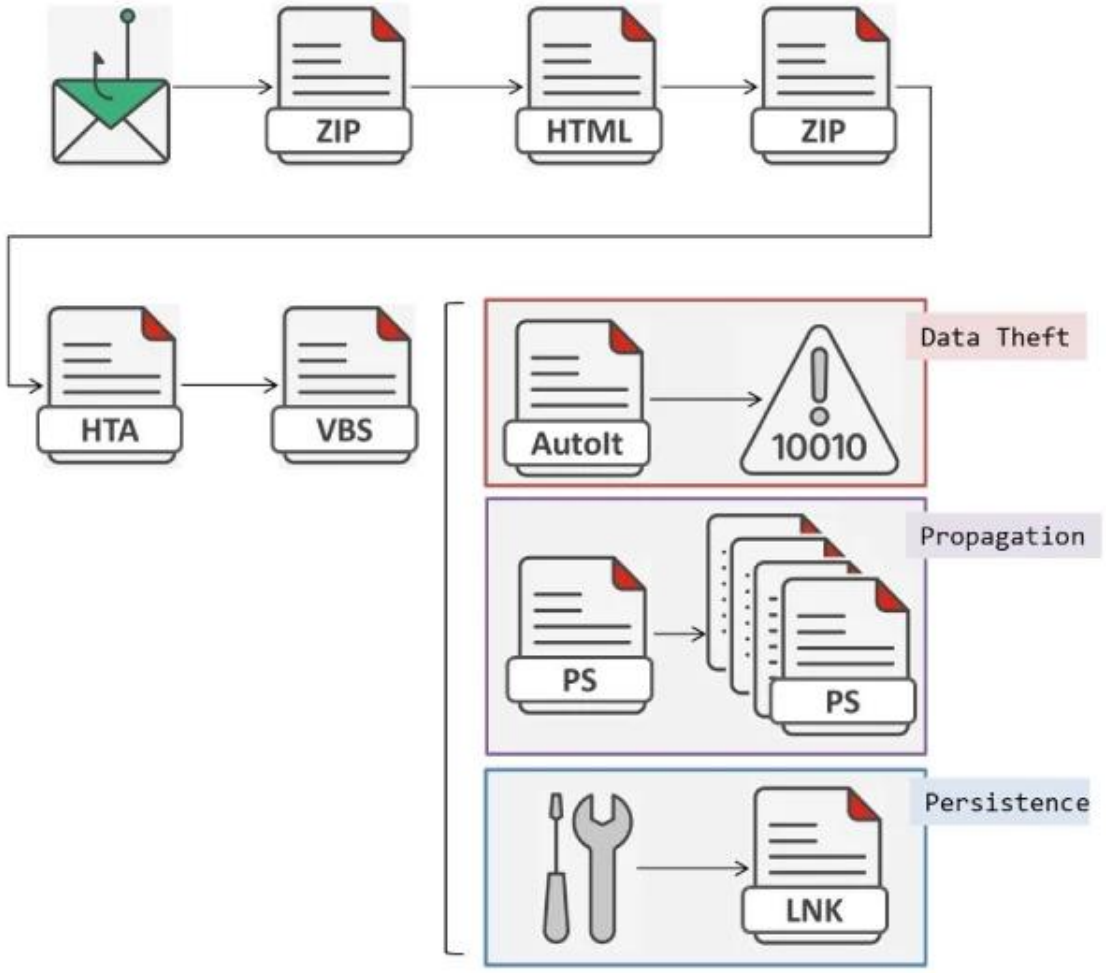
Investigadores en ciberseguridad han detectado una nueva campaña de phishing utilizada para distribuir un malware llamado Horabot, dirigido a usuarios de Windows en países latinoamericanos como México, Guatemala, Colombia, Perú, Chile y Argentina.

> Según la investigadora Cara Lin de Fortinet FortiGuard Labs, esta campaña *«utiliza correos electrónicos manipulados que se hacen pasar por facturas o documentos financieros para engañar a las víctimas y hacer que abran archivos adjuntos maliciosos. Esto permite robar credenciales de correo electrónico, extraer listas de contactos e instalar troyanos bancarios».*

La actividad fue observada por la empresa de seguridad en redes en abril de 2025, enfocándose principalmente en usuarios de habla hispana. También se ha identificado que los atacantes envían mensajes de phishing desde las propias cuentas comprometidas de las víctimas usando automatización de Outlook mediante COM, lo que facilita la propagación lateral del malware dentro de redes corporativas o personales.



Además, los responsables de esta campaña ejecutan varios scripts en VBScript, AutoIt y PowerShell con el fin de realizar un reconocimiento del sistema, sustraer credenciales y desplegar cargas maliciosas adicionales.

Horabot fue documentado por primera vez por Cisco Talos en junio de 2023, aunque se ha rastreado su actividad desde al menos noviembre de 2020, enfocándose en usuarios hispanohablantes en América Latina. Se cree que el grupo detrás de estas operaciones tiene origen en Brasil.

El año pasado, Trustwave SpiderLabs también reveló otra campaña de phishing en la misma región que distribuía cargas maliciosas similares a las del malware Horabot.

La nueva oleada de ataques comienza con un correo electrónico de phishing que utiliza señuelos con temática de facturación para convencer al usuario de abrir un archivo comprimido ZIP que supuestamente contiene un documento PDF. Sin embargo, en realidad, el archivo contiene un archivo HTML malicioso con datos codificados en Base64 que intenta conectarse a un servidor remoto para descargar una carga adicional.

Esa nueva carga consiste en otro archivo ZIP, dentro del cual se encuentra una aplicación HTML (HTA) que ejecuta un script alojado en un servidor externo. Este script inyecta un VBScript externo que realiza varias verificaciones para abortar su ejecución si detecta la presencia del antivirus Avast o si se encuentra en un entorno virtual.

Posteriormente, el VBScript recoge información básica del sistema, la envía a un servidor remoto y descarga más cargas maliciosas, incluyendo un script AutoIt que lanza el troyano bancario mediante una DLL maliciosa, así como un script en PowerShell encargado de propagar correos de phishing. Este último recopila direcciones de correo escaneando los contactos almacenados en Outlook.

> *«El malware luego roba datos relacionados con la actividad del navegador desde una variedad de navegadores específicos, incluyendo Brave, Yandex, Epic Privacy Browser, Comodo Dragon, Cent Browser, Opera, Microsoft Edge y Google Chrome. Además del robo de datos, Horabot monitorea el comportamiento del usuario e inyecta ventanas emergentes falsas diseñadas para capturar credenciales sensibles de acceso del usuario»*, explicó Lin.